



Acceptable Use Policy
V2.2 01/23

Acceptable Use Policy

Our Acceptable Use Policy (“AUP”) is provided to give our customers and third parties a clear understanding of what we expect of them whilst using our service. All users, including those who have been given access for the purposes of demonstration, support and as a sales tool, as well as those who pay a fee to subscribe to our services, must comply with this AUP and also our TOS (Terms of Service).

Use of our service(s) constitutes acceptance and agreement to our AUP as well as our TOS (Terms of Service)

We support the uncensored flow of information and ideas over the Internet and do not actively monitor subscriber activity under normal circumstances. We reserve the right to exercise editorial control over content that can be accessed through our service. We may remove any materials that, in our sole discretion, may be illegal, may subject us to liability, or may violate this AUP. We may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrongdoing. Your violation of this AUP may result in the suspension or termination of either your account or other actions as detailed below WITHOUT PRIOR NOTIFICATION.

This document is intended to provide a basic understanding of our AUP. The following are guidelines for the establishment and enforcement of our AUP:

- Ensure reliable service to our customers
- Ensure security and privacy of our systems and network, as well as the networks and systems of others
- Comply with existing laws
- Maintain our reputation as a responsible and reliable Service Provider
- Preserve the privacy and security of individual users
- You may not use your account to publish, send, receive, transmit or store material which we deem to be unlawful, offensive, defamatory or indecent. For purposes of this policy, “material” refers to all forms of communications including, but not limited to narrative descriptions, graphics (photographs, illustrations, images, drawings, logos), executable programs, video recordings, and audio recordings.

If your account is used to violate the AUP, we reserve the right to terminate your service(s) without notice.

We abide by any ‘notice and take down’ recommendations issued by the Internet Watch Foundation.

If you have any questions regarding this policy, please contact us at support@virtualsignature.net

VIOLATIONS OF THE AUP

The following constitute violations of this AUP:

- **Illegal use:** Our services may not be used for illegal purposes or to commit any actionable breach of a third party’s rights under the law, or for transmission of illegal or harmful materials, or in support of illegal activities. We reserve the right to cooperate with legal

authorities and/or injured third parties in the investigation of any suspected crime or civil wrongdoing.

- Harm to minors: Use of the services to harm, or attempt to harm, minors in any way, including, but not limited to child pornography.
- Threats: Use of the services to transmit any material (by e-mail, uploading, posting or otherwise) that threatens or encourages bodily harm or destruction of property or otherwise threatens any person.
- Harassment: Use of the services to transmit any material (by e-mail, uploading, posting or otherwise) that harasses another.
- Fraudulent activity: Use of the services in any form of fraudulent activity, including without limitation to make fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as "pyramid schemes," "ponzi schemes," and "chain letters."
- Forgery or impersonation: Adding, removing or modifying information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forgery is prohibited.
- Unsolicited commercial e-mail / unsolicited bulk e-mail (SPAM): Use of the services to transmit any unsolicited commercial or unsolicited bulk e-mail or collect responses thereto is expressly prohibited. Violations of this type will result in the immediate termination of the offending account.
- E-mail / News Bombing: Malicious intent to impede another person's use of electronic mail services or news will result in the immediate termination of the offending account.
- E-mail / Message Forging: Forging any message header, in part or whole, of any electronic transmission, originating or passing through the services is a violation of this AUP.
- Unauthorized access: Use of the services to access, or to attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of our or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data, is expressly prohibited and the offending account is subject to immediate termination.
- Infringement of Proprietary Rights: Use of the services to transmit or distribute any material (by e-mail, uploading, posting, hot linking, directly linking or otherwise) that infringes any copyright, trademark, patent, trade secret, confidentiality, privacy or other proprietary rights of any third party, including, but not limited to, the unauthorised copying of copyrighted material, the digitisation and distribution of photographs from magazines, books, or other copyrighted sources, and the unauthorised transmittal of copyrighted software.
- Collection of personal data: Use of the services to collect, or attempt to collect, personal information about third parties without their knowledge and/or consent or otherwise in a way that is not in accordance with applicable Data Protection, GDPR or other legislation and guidance from regulatory authorities.
- Network disruptions and unfriendly activity: Use of the services for any activity which affects the ability of other people or systems to use our services or the internet. This includes without limitation "denial of service" (DOS) attacks (including flooding of systems, deliberate attempts to overload a service or attempts to crash a host) or network scans against another network host or individual user, the sending of data with forged addresses, sudden increase in your use of network capacity that impacts other users on the network or configuration of PCs as an open relay system. Interference with or disruption of other network users, services or equipment is prohibited. It is your responsibility to ensure that their network is configured in a secure manner. You may not, through action or inaction, allow others to use your network for actions in breach of this AUP. You may not permit your network, through action or inaction, to be configured in such a way that gives a third party the capability to use their network in breach of this AUP. Unauthorised entry and/or use of another company

and/or individual's computer system will result in immediate account termination. We will not tolerate any subscriber attempting to access the accounts of others, or penetrate security measures of other systems, whether or not the intrusion results in corruption or loss of data. You must ensure that any system you connect to the Internet conforms to all applicable Internet Engineering Task Force (IETF) standards.

- **Fraud:** Involves a knowing misrepresentation or misleading statement, writing or activity made with the intent that the person receiving it will act upon it.
- **Distribution of Viruses:** Distribution or storage of software that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems are prohibited. This will result in the immediate termination of the offending account.
- **Mailboxes and Mailing Lists:** You must ensure that your use of mailboxes does not adversely affect the proper functioning of our systems, including where mailboxes:
 - receive large volumes of undeliverable mail;
 - have forwarders set to other mailboxes where mail cannot be delivered, or have forwarders or auto-responders that generate circular loops.

If you run a mailing list using our services, you should comply with Linux Current Best Practice. You are responsible for keeping records to show that each subscriber has given their consent to their inclusion on the mailing list.

- **News Groups:** You must not breach any guidelines or restrictions of any news group. The following are expressly prohibited
 - excessive cross-posting, posting of irrelevant material or advertisements;
 - posting binaries to non-binary news groups.
- **Storage:** Web-space may be used for any legitimate website content but must not be used to store backups, downloads, archives or other non-web based content. Streamed multimedia content such as audio and video is acceptable, but links to HTTP download of this content is prohibited. You must only use scripts to produce web-based content.
- **Pornography:** You must not distribute, transmit or store any material that is defamatory, obscene, indecent, pornographic on the service,

SECURITY

You are responsible for any misuse of your account, even if the inappropriate activity was committed by a third party, including without limitation a friend, family member, guest, director, officer, agent, contractor or employee. Therefore, you must take steps to ensure that others do not gain unauthorised access to your account. In addition, you may not use your account to breach security of another account or attempt to gain unauthorised access to another network or server.

Your password provides access to your account. It is your responsibility to keep your password secure.

Sharing your password and account access with unauthorised users is prohibited. You should take care to prevent others from using your account since you will be held responsible for such use.

Attempting to obtain another user's account password is strictly prohibited, and may result in termination of service.

You must adopt adequate security measures to prevent or minimise unauthorised use of your account.

You may not attempt to circumvent user authentication or security of any host, network or account. This includes, but is not limited to, accessing data not intended for you, logging into or making use of an account you are not expressly authorised to access, or probing the security of other networks. Use or distribution of tools designed for compromising security is prohibited. Examples of these tools include, but are not limited to, password guessing programs, cracking tools or network probing tools.

Users who violate systems or network security may incur criminal or civil liability. We will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities in the investigation of suspected criminal violations.

NETWORK PERFORMANCE

Accounts operate on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited by this policy and may result in termination of your account.

FAIR DATA/BANDWIDTH USAGE

We operate a Fair Data Usage Policy to ensure our customers enjoy the best possible digital signature and document exchange service. To make sure everything is running smoothly and to allow us to detect excessive use, we continuously monitor data usage in order to maintain a consistent level of network quality and service to all our customers.

Our Fair Data Usage is measured by the number of transaction and SecureCode SMS credits used per transaction. On occasions, some customers require a higher level of data exchange at any one time, which is acceptable, provided the overall data exchange credits used are kept within the Fair Data Usage terms of their licence. The number of data exchange credits are confirmed on each licence and may be increased by arrangement.

The vast majority of our customers use this service considerately and their data usage levels do not disproportionately affect the shared network exchange capacity. Our Fair Data Usage Policy manages inappropriate use and makes sure the service can be used fairly by everyone.

Although our Fair Data Usage Policy applies to all our customers, it will only affect the very few customers who make inappropriate use of our service. Where you are in breach of the Fair Data Usage Policy we may contact you to discuss changing your licence so that it conforms to the Fair Data Usage Policy, but reserve the right to do one or more of the following;

- Suspend your service until data credit terms of your licence have been amended;
- Terminate your service by giving you not less than 14 days prior written notice;
- Amend our Fair Usage Policy at any time without advanced warning or notice.

REPORTING VIOLATIONS OF VIRTUALSIGNATURE-ID'S AUP

We request that anyone who believes that there is a violation of this AUP direct the information to the Support Department at support@virtualsignature.com

If available, please provide the following information:

- The IP address used to commit the alleged violation
- The date and time of the alleged violation, including the time zone or offset from GMT
- Evidence of the alleged violation

E-mail with full header information provides all of the above, as do system log files. Other situations will require different methods of providing the above information. We may take any one or more of the following actions in response to complaints:

- Issue written or verbal warnings
- Suspend the account
- Terminate the account
- Bill the account holder for administrative costs and/or reactivation charges
- Bring legal action to end violations and/or to collect damages, if any, caused by violations

CONTACT

You are responsible for keeping your contact details with us up to date. Where we are unable to contact you at an address you have given, we will reserve the right to suspend or terminate your service by giving 30 days written notice to the last known address.

REVISIONS TO THIS ACCEPTABLE USE POLICY

We reserve the right to revise, amend, or modify this AUP, our TOS and our other policies and agreements at any time and in any manner. Notice of any revision, amendment, or modification will be posted in accordance with our TOS.